PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Data Breaches

Notification Practices

Over the past year, businesses have learned numerous lessons about data breaches. This article highlights ten common mistakes to avoid when responding to a data breach incident.

Ten Common Mistakes in Responding to a Data Breach Incident

BY REECE HIRSCH

One year after the ChoicePoint incident cast a spotlight on security breach notification issues, a few lessons have been learned by businesses responding to, or seeking to avoid, data breach incidents. Some of these lessons have been learned the hard way by companies that have experienced negative publicity, state attorney general and Federal Trade Commission scrutiny, declining stock prices, and class action lawsuits.

As the saying goes, those who do not learn from history are doomed to repeat it. This article outlines ten common mistakes to avoid in responding to data breach incidents.

1. ***Overreacting***. Once a company has sent a security breach notice to its customers, it is impossible to ''unring the bell.'' On the other hand, statutes such as California's S.B. 1386 require notification ''in the most expedient time possible and without unreasonable delay.'' These two competing imperatives may be balanced only if a company is prepared to conduct a thorough investigation of a potential data breach immediately upon becoming aware of an incident.

For example, one client company learned that a laptop containing a wealth of confidential customer data was missing. The company commenced preparations to notify its customers around the country. At the same time, the company launched a vigorous internal investigation that included questioning of a security guard who had access to the laptop. The security guard soon confessed that he had hidden the missing laptop within the company's offices with the intention of removing it later. The company had no reason to believe that the laptop had ever left the premises or that the data had been accessed by an unauthorized person. The company was fortunate because it was able to bring its investigation to a prompt and successful conclusion before sending more than a million notice letters to customers.

Reece Hirsch, a partner in the San Francisco office of Sonnenschein Nath & Rosenthal LLP, specializes in privacy and data security issues. He can be reached at (415) 882-5040 or rhirsch@sonnenschein.com.

2. ***Failing to Adopt a Security Compliance Program, Including an Incident Response Plan.*** In the past few years the framework of data security laws, regulations, and industry standards has evolved, and now includes state security breach notification laws, the Payment Card Industry (PCI) Data Standard, the Gramm-Leach-Bliley Act safeguards rules, the FTC's regulation of security practices under the ''unfairness'' doctrine, California's ''reasonable security procedures and practices'' law (A.B. 1950), the federal bank regulatory agencies' guidance on consumer data breaches, and the Health Insurance Portability and Accountability Act (HIPAA) security rule. As a prudent risk management practice and to comply with these new legal and industry standards, it is important for companies to conduct a formal information security risk assessment and adopt written policies and procedures based upon the findings of that assessment. A data breach incident response plan is an integral part of any comprehensive security compliance program.

As noted above, state security breach notification laws generally require notices to be sent very promptly. In a guidance document, the California Office for Privacy Protection recommended that notices be sent within ten business days. In order to respond in such an expedited manner, particularly given the complex logistics of printing and mailing a mass notification, it is vital to have an incident response plan. Precious days can be lost if a company is forced to formulate its approach on the fly.

3. ***Failing to Follow an Incident Response Plan.*** In the heat of a crisis, companies sometimes neglect to follow the security incident response plan that they have adopted. If a company's response to a data breach incident later comes under scrutiny by regulators or the plaintiffs in a class action lawsuit, the company generally will be well-served if it can demonstrate that its response was reasonable. The easiest way to demonstrate that a company failed to act reasonably is to show that it adopted prudent, industry-standard security incident response policies and procedures—and then failed to follow them.

4. ***Not Training Your Personnel to Spot Data Breaches.*** To many within an organization, the theft of a laptop may not seem like a major event. However, if that laptop contains the Social Security numbers of all of a company's customers, the theft, if not properly handled, could have a catastrophic impact on the future of the company. One of the most important aspects of a security compliance program is educating employees so that they can identify and promptly report to their supervisors potential data breach incidents.

One of the worst situations to be faced with under state security breach notification laws is learning of an incident too late. Occasionally, an employee will report an incident, such as the theft of a laptop containing personal information, to their immediate supervisor. If the employee and supervisor are not sensitized to data breach issues, weeks may pass before the privacy officer or management become aware that a potential data breach has occurred. At that point, the company is faced with the unpleasant prospect of being legally required to report to its customers an incident in which the company has clearly failed to comply with the applicable security breach notification law.

5. ***Failing to Follow Forensic Procedures.*** For breaches that involve identity thieves or other wrongdoers, the ideal outcome is the apprehension of the perpetrator and the recovery of the data before customers are harmed. Failure to follow proper computer forensic procedures may erase or spoil the evidence that could lead to prosecution or apprehension of such criminals. Companies should identify internal or external computer forensic resources in advance so that they can be mobilized quickly when a breach occurs. If the company intends to utilize external forensic consultants, internal IT staff should receive training regarding proper coordination with the consultants and avoiding destruction and contamination of evidence.

For example, by starting an investigation and reviewing the systems directly without first making a forensic image, you risk changing the ''access'' and ''modified'' dates (both a form of metadata) of the relevant files. Once you do that, you can't prove when they were last accessed or modified, and can't match the forensic image up with logs that may show a hacker's IP address. By first making a forensic image, you preserve everything—including the metadata—so you can return to that ''snapshot'' at any time.

6. ***Inadequate Management of Vendor Relationships***. California's S.B. 1386 requires that any person or business that maintains computerized data that includes personal information that it does not own must notify the owner or licensee of the information immediately upon learning of a security breach. A company that entrusts its customer information to third party vendors should make sure the vendors understand this legal obligation. It is also advisable to require the vendor to notify the company of the breach within a specified time frame (*i.e.*, 24 hours or 2 business days). In certain cases, it may also be prudent to specify in the vendor agreement a process for coordinating with respect to breach notification and the content of the notice letter.

7. ***Failing to Coordinate Effectively With Credit Reporting Agencies.*** When a security breach incident occurs, the company should consider notifying credit reporting agencies before sending a notice to customers. If a police report has been filed, customers may find it useful to receive a copy of that report along with the breach notification. Having a copy of the police report in hand may make it easier for customers to reference the incident when communicating with credit reporting agencies. Companies should also consider offering free credit reporting for a specified period (*i.e.*, one year) to affected customers.

8. ***Failing to Coordinate Effectively With Law Enforcement Authorities***. S.B. 1386 and most other state security breach notification laws provide that notification may be delayed if a law enforcement agency determines that notification will impede a criminal investigation. A company should not delay notifying customers based upon such provisions unless they receive strong confirmation, preferably in writing, from the relevant law enforcement agency that the notice would impede the investigation.

A company should carefully consider the appropriateness of notifying law enforcement of an incident, as well as which agency might most aggressively pursue the case. A routine laptop theft may or may not receive prolonged attention from the local police department. However, if the breach is the work of a sophisticated ring of hackers, then the case might be attractive to the local high tech crimes task force, the FBI, the Secret

  PVLR ISSN 1538-3423

Service, or the National Infrastructure Protection Center.

9. ***Forgetting That State Security Breach Notification Laws Differ.*** California's S.B. 1386 was the first security breach notification statute and it remains a model for many other state laws. However, some security breach notification laws differ from S.B. 1386 in significant respects. For example, under the security breach notifications laws of certain states (such as New Jersey, New York and North Carolina) specified state agencies must be notified of the breach, in addition to the consumer. Other states (including Georgia, Maine, Minnesota, Montana and Nevada) require notification of credit reporting agencies. A company experiencing a security breach should review the security breach notification laws of all states in which personal information has been compromised and formulate an incident response that complies with all applicable notification laws.

10. ***Lawyers and IT Personnel Must Speak a Common Language.*** Terms such as ''breach'' and ''access'' can have very different meanings when spoken by lawyers, IT personnel, and company executives. Developing an incident response team in advance allows the participants to make sure they are speaking a common language before the bullets begin flying. For example, a phishing scheme might be loosely referred to as a breach, when it actually does not constitute a breach triggering notice under state security breach notification laws. A typical phishing scheme does not involve the unauthorized acquisition of data maintained by the company. Instead, it usually involves the use of deception to obtain a user ID and password from the customer. A security incident response team should bring to bear, in a coordinated fashion, all of the skills needed to effectively respond to a data breach crisis, which may include personnel from legal, information technology, management, compliance, public relations, investor relations, and human resources.